REMARKS

The application has been amended and is believed to be in condition for allowance.

Amendments to the Disclosure

Claim 1 is amended to further recite cryptographic means for authenticating the sender of the command, based on the subject matter of claim 2. Claim 2 is canceled without prejudice. The amendment finds support in the specification and the drawing figures as originally filed (e.g., page 8, lines 10-12).

Claim 3 is amended to depend from and correspond to amended claim 1. Amended claim 3 finds support in the specification and the drawing figures as originally filed (e.g., page 3, lines 14-19; page 8, lines 10-14)

Claim 13 is amended to incorporate the subject matter of claim 14, and finds support in the specification and the drawing figures as set forth above as to the amendments to claims 1 and 3. Claim 14 is canceled without prejudice.

Claims 1-23 are further amended with formal revisions in consideration of U.S. practice and preferences.

The amendments to the claims do not introduce new matter.

The specification is amended to include section headings; the amendment to the specification does not introduce new matter.

Formal Matters - Information Disclosure Statement

The Official Action stated that the NPL document on the Information Disclosure Statement ("IDS") filed April 4, 2005 fails to comply with 37 CFR 1.98(a)(3) because it does not include a concise explanation of the relevance of each patent listed that is not in the English language.

Applicants note the Official Action's statement as to the IDS. However, it is respectfully submitted that the IDS of April 4, 2005 was filed as part of a Foreign Search Report as to PCT/FR/03/02854, and that the NPL document XP-002243893 is listed as the first item of page 2 of the Report, and includes an indication of relevance consistent with MPEP § 609.04(a), section III, paragraph 2.

Accordingly, it is respectfully submitted that the IDS of April 4, 2005 is compliant with 37 CFR 1.98(a)(3). Consideration of NPL document XP-002243893 is thereby respectfully requested.

Substantive Issues - Section 102 and 103

The Official Action rejected claims 1, 5-7, 9, 13, 16-17, and 20 under 35 USC 102(b) as being anticipated by Armuzzi et al. (EP 1 143 688; "ARMUZZI") as cited in the present application.

The Official Action rejected claims 1-4, 10-11, 13-15, and 21-22 under 35 USC 102(b) as being anticipated by

Sloan (US 6,273,335; "SLOAN") as cited in the present application.

The Official Action rejected claims 12 and 23 under 35 USC 103(a) as being unpatentable over SLOAN in view of Lin et al. (EP 1 223 565; "LIN") as cited in the present application.

The Official Action rejected claims 8 and 18-19 under 35 USC 103(a) as being unpatentable over SLOAN in view of Sato (US Pub. 2002/0103891; "SATO").

The rejections are respectfully traversed for at least the reasons that follow.

It is firstly noted that claims 1 and 13 have been amended, as indicated above. It is respectfully submitted that none of the references cited, individually or in combination, teach or suggest the invention as presently recited in claims 1 and 13 as amended.

The Official Action offered SLOAN as anticipating the subject matter recited by original dependent claims 2 and 14, now incorporated into independent claims 1 and 13. The Official Action contends that SLOAN teaches a means for authenticating the sender of said command (at Abstract, and column 6, lines 36-49, stating that the command includes the password and CID number of the owner of the card).

It is respectfully submitted that SLOAN neither teaches nor suggests cryptographic means for authentication,

as required by amended claims 1 and 13. At best SLOAN teaches authenticating an unlocking command only in comparing two passwords; that is, a memorized password and a received password are compared. No cryptographic means is taught as part of this process.

SLOAN teaches locking an application with steps comprising i) transmitting a locking command, from the device to the smart card, ii) locking the application in the smart card, iii) transmitting the smart card identifier and password, from the smart card to the device, and iv) memorizing the identifier and password in the device (see, e.g., SLOAN Figure 8; column 7, lines 33-59).

Unlocking an application, as described by reference to Figure 12 of SLOAN, comprises i) reading the identifier of a smart card in the device, and ii) determining whether a password associated to the smart card identifier has been previously memorized (column 8, lines 51-65).

If a password associated to the smart card identifier has been previously memorized, SLOAN proceeds to i) transmit an unlocking command comprising the previously memorized password from the device to the smart card, and ii) comparing the received password with the smart card password and unlocking the application if both passwords are similar (Figure 12; column 8 line 66 to column 9 line 13).

SLOAN makes no teaching of any cryptographic means or step. Authenticating the unlocking command in the SLOAN's smart card consists in comparing two passwords, that is to say a memorized password and a received password, without using any cryptographic means.

At best, SLOAN refers loosely to cryptographic algorithms (column 6, lines 24 to 35) used to generate a password for storage on the card, prior to use of the card and outside the smart card (e.g., generating a key according to a known algorithm by an agent of the card issuer, based on a card number and a master key during initialization; see column 6, lines 8-24), and not for authenticating the sender of a command received by the smart card.

Likewise, the reference to ISO 7816-4 (column 8, lines 9 to 17) concerns the command format, and not its decrypting.

Further, SLOAN teaches that data transmission between the smart card and the device is a direct transmission; that is, data is not disclosed as transmitted over a system of a third-party constituting a security vulnerability for data transmitted "in the clear". Similarly, the device should belong to a trusted party since it is not secured by itself (column 6, lines 50 to 52). Thus, SLOAN makes no suggestion of any need for encryption for data exchanged between the device and the smart card.

Moreover, if data to be exchanged between the device and the smart card were to be encrypted, it would have been necessary in SLOAN for the device and the smart card to memorize complementary encryption and decryption keys (e.g., private or public/private keys). Such keys would be exchanged between the device and the smart card or be received from the system of a third party. As the device according to SLOAN is stand-alone, the keys cannot be received from the system of a third party. Therefore, the keys would have to be exchanged between the device and the smart card.

However, exchanging cryptographic keys between two entities for encrypting data that should be exchanged afterwards does not significantly secure the data transmission, because the cryptographic keys may be accessed by an eavesdropping third party if the data itself can be accessed by such a third party. Therefore, encrypting data using exchanged encryption keys does not significantly increase transfer security of the data.

As a consequence, not only is data encryption for data exchange between the device and the smart card not disclosed within SLOAN, either explicitly or implicitly, it is plain that one skilled in the art would not have implemented such a feature that increases complexity without improving data transfer security.

Thus, it is respectfully submitted that SLOAN fails to either teach or even suggest cryptographic means or use of same for authenticating the sender of a command as required by the invention as recited in the amended independent claims.

Withdrawal of the rejection over SLOAN is respectfully solicited.

It is also respectfully submitted that no combination of SLOAN with any other of the cited references teaches or suggests the invention as claimed.

For example, LIN fails to overcome the deficiencies of SLOAN. LIN is directed to a mutual authentication of a terminal and a smart card for transaction purpose. For at least the reasons discussed above, one skilled in the art would not combine the teaching of this document with SLOAN.

However, even if the teaching of SLOAN were to be modified with that of LIN, the result, at best, would have been a smart card adapted to cooperate with a device allowing the locking and unlocking of applications, according to the teaching of SLOAN, and adapted to operate a mutual authentication with a terminal prior to exchange data. Hence the claimed invention would not be obtained.

It is therefore respectfully submitted that independent claims 1 and 13 are patentable over the cited references.

It is further respectfully submitted that claims depending from claims 1 and 13 are patentable at least for depending from a patentable parent claim.

Reconsideration and allowance of the claims are respectfully requested.

From the foregoing, it will be apparent that Applicants have fully responded to the February 11, 2009 Official Action and that the claims as presented are patentable. In view of this, Applicants respectfully request reconsideration of the claims, as presented, and their early passage to issue.

In order to expedite the prosecution of this case, the Examiner is invited to telephone the attorney for Applicants at the number set forth below if the Examiner is of the opinion that further discussion of this case would be helpful.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON

/Jeremy G. Mereness/

Jeremy G. Mereness, Reg. No. 63,422
209 Madison Street
Suite 500
Alexandria, VA 22314
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

JGM/fb